World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(Review Article)

Security aspects in IoT based cloud computing

Ehsan Bazgir [1, *], Ehteshamul Haque [2], Numair Bin Sharif [3] and Md. Faysal Ahmed [4]

[1] Department of Electrical Engineering, School of Engineering, San Francisco Bay University, Fremont, CA 94539, USA.
[2] Department of Computer Science, School of Engineering, San Francisco Bay University, Fremont, CA 94539, USA.
[3] Department of Computer Science and Engineering, United International University, Dhaka 1212, Bangladesh.
[4] Shaikh Borhanuddin Postgraduate College, Affiliated by National University, Dhaka-1100, Bangladesh.

World Journal of Advanced Research and Reviews, 2023, 20(03), 540–551

Publication history: Received on 27 October 2023; revised on 04 December 2023; accepted on 06 December 2023

Article DOI: https://doi.org/10.30574/wjarr.2023.20.3.2481

Abstract

Cloud computing offers a flexible framework in which data and resources are spread across different locations and can be accessed from various industrial environments. This technology has revolutionized the way resources such as data, services, and applications are used, stored, and shared in industrial applications. Over the past decade, industries have rapidly embraced cloud computing due to its advantages of enhanced accessibility, cost reduction, and improved performance. Moreover, the integration of cloud computing has led to significant advancements in the field of the Internet of Things (IoT). However, this quick shift to the cloud has also introduced various security concerns and challenges. Traditional security solutions are not always suitable or effective for cloud-based systems. Despite the continuous use of complex cyber weapons, efforts have been made in recent years to address the security issues and concerns associated with cloud platforms. The rapid progress of deep learning (DL) in the field of artificial intelligence (AI) has provided opportunities to tackle these security challenges in the cloud. The research presented in this study encompasses a comprehensive survey of the enabling architecture, services, configurations, and security models for cloud-based IoT. It also categorizes the security concerns in IoT within four major categories (data, network and service, applications, and people-related security issues) and provides a detailed discussion on each category. Furthermore, the study examines the latest advancements in cloud-based IoT attacks, analyzes significant security issues within each category, and presents the limitations from a broader perspective encompassing general, artificial intelligence, and deep learning aspects.

Keywords: Cloud Computing; IoT Security; Cybersecurity; Attack Prevention; Platform as a Service (PaaS); Infrastructure as a Service (IaaS); Software as a Service (SaaS)

1. Introduction

An extensive network consisting of various IoT-supported applications and devices is known as an internet of things (IoT)-based cloud infrastructure. This infrastructure encompasses servers, storage, underlying infrastructure, real-time processing, and operations. Moreover, it includes standards and services that are crucial for securing, managing, and connecting different IoT applications and devices. The typical IoT architecture is illustrated in Figure 1, while Figure 2 provides an overview of the IoT-based cloud attack model. Over the past decade, the cloud has gained prominence, and its different forms continue to grow in the new decade [1, 2, 3, 4, 5].

[*] Corresponding author: Ehsan Bazgir

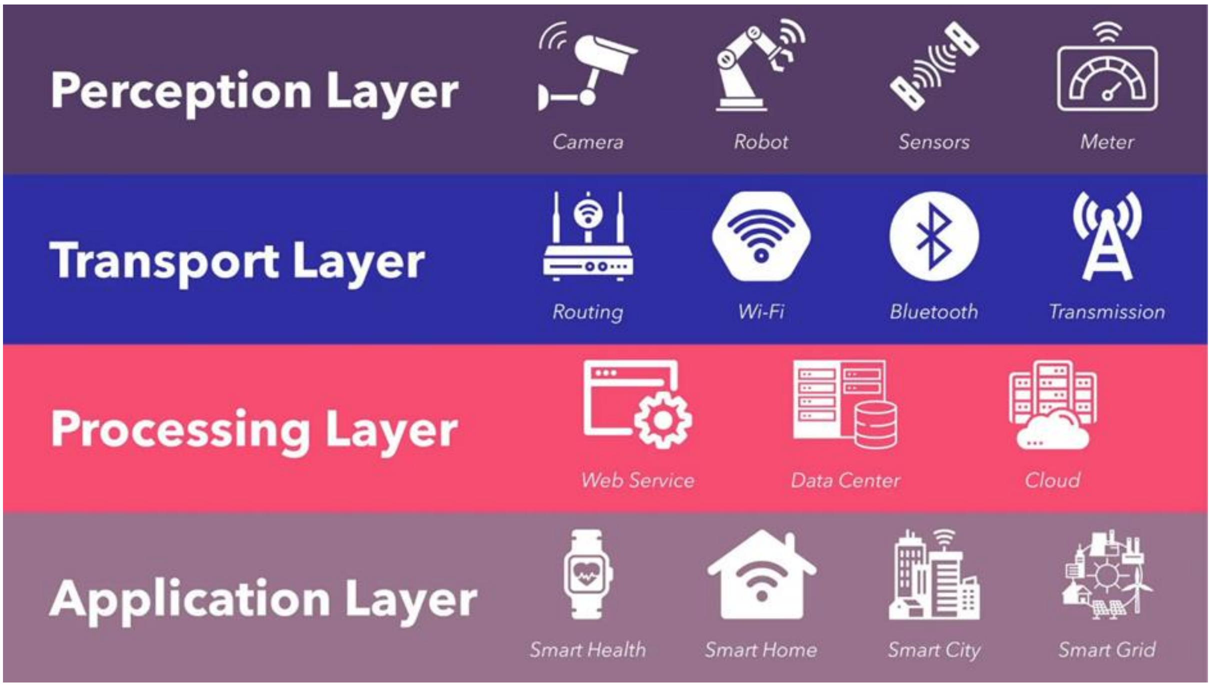


Figure 1 IoT Architecture (Adopted from https://dgtlinfra.com/internet-of-things-iot-architecture/)

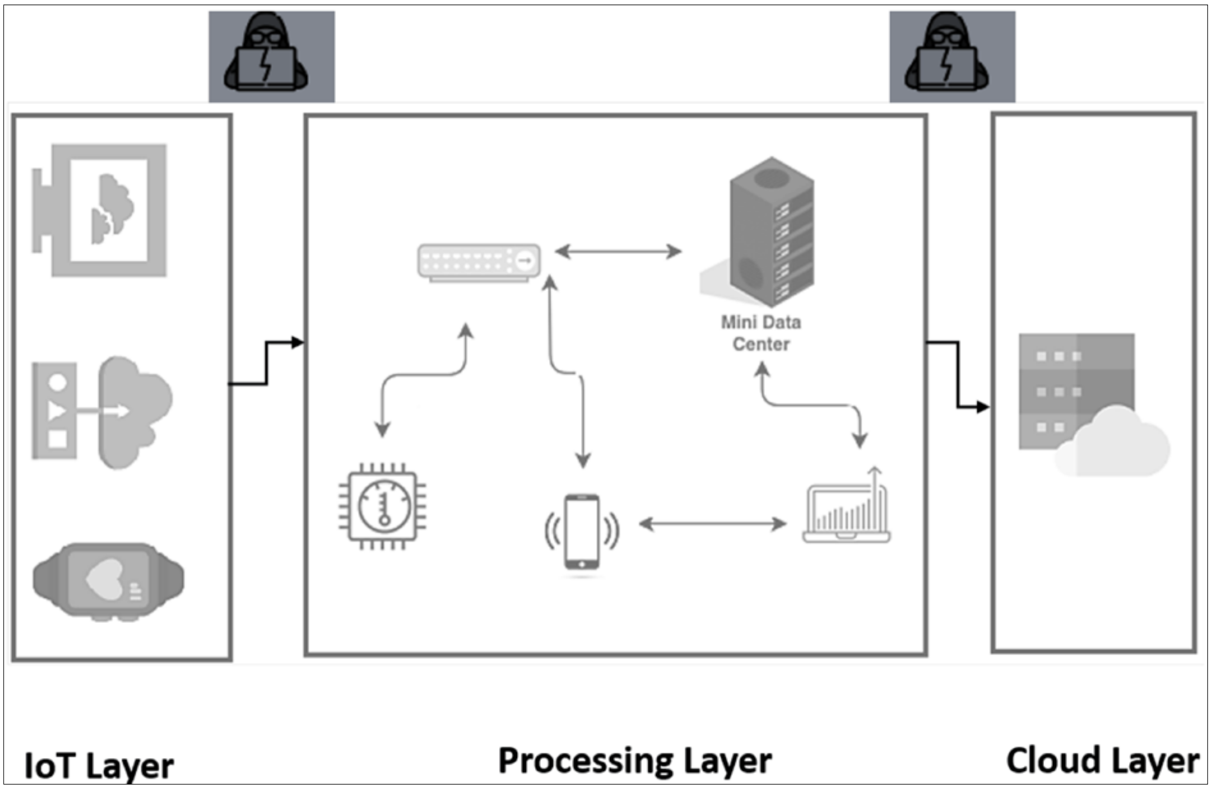


Figure 2 IoT-based cloud attack model (Adopted from [1])

The National Institute of Standards and Technology (NIST) has identified five key characteristics of cloud computing [6]. These characteristics include measured service, resource pooling, rapid expansion, network access, and on-demand self-service. Additionally, cloud services are delivered through four deployment models and three service models [7]. The primary objective of cloud computing is to offer various computing services, such as servers, storage, databases, networking, software, analytics, and intelligence, over the internet. Users can access and utilize these services according to their specific requirements [8-11]. The migration of traditional IT services to the cloud has been driven by factors such as cost effectiveness, convenience, flexibility in work, and efficient data storage and retrieval. Cloud computing eliminates the need for industries to invest in expensive hardware and software for on-site data centers. Instead, cloud technologies enable industries to automate their processes by storing software systems and services on remote servers. This trend has gained significant traction across industries and continues to grow steadily each year [12].

Cloud service providers (CSPs) offer amazing software-as-a-service (SaaS), platform-as-a-service (PaaS), and infrastructure-as-a-service (IaaS) models that are widely recognized. These services provide incredible features like data storage, resource sharing, and virtual computing. By offering virtual servers, launching virtual data centers, and executing software applications, CSPs cater to both private, public, and hybrid cloud environments. What's even more exciting is that users and software developers can fully utilize these services without having to worry about the technical aspects of managing their own infrastructure. However, it's important to note that when transferring data and applications from the user's environment to the cloud environment, there may be some security risks involved. Since cloud services are launched and provided on the internet infrastructure, there is a possibility of Internet-based threats affecting these services. But don't worry, CSPs prioritize security and take measures to mitigate these risks. It's just that the data still needs to be transmitted through the internet, which may not be entirely secure. Nonetheless, the benefits and opportunities offered by cloud computing services are absolutely incredible [13].

The cloud provides a means for distributing diverse data and resources through virtual environments. Unlike traditional business software infrastructures, cloud computing allows users access to unlimited storage space and increased server resources as needed. However, conventional methods for user identification, authentication, and access management are not entirely adaptable to the cloud. Security concerns arise from external data storage, limited user control, and integrated models. The paramount worry in cloud-based systems revolves around safeguarding data, as its compromise can lead to various cybercrimes affecting individuals, organizations, and even states [14].

Common threats in cloud security include crypto-jacking, denial of service, account theft, and data breaches. According to a report by Skybox Security in 2019, there was a significant surge in vulnerabilities within cloud containers compared to traditional storage architectures. Cloud providers primarily secure the platform, leaving customer data vulnerable. The Oracle and KPMG Cloud Threat Report of 2019 revealed that 82% of cloud users experienced security events [15, 16]. Consequently, ensuring robust security and privacy measures in the cloud has become imperative. Security is a critical factor for the success of cloud computing, with data location identified as a concern in 2011. Ongoing discussions have centered on data security concerns. Trust is another focal point, directly tied to the credibility of cloud service providers. Researchers emphasize the importance of trust models and management in addressing inherent security issues in cloud computing [17-20].

2. Related Works

Cloud computing (CC) has experienced significant growth in recent years. Numerous studies have delved into the realm of security threats, vulnerabilities, issues, challenges, and countermeasures. This section covers the security issues related to cloud computing.

In [21], the authors delve into the intricacies of cloud computing, exploring its structures, security threats, and the corresponding solutions. The study also discussed current deployment models, cloud services, and cloud architecture frameworks, along with the assisting technologies. This study's findings were utilized to pinpoint future research areas in cloud security. In a separate publication, the authors emphasized the significance of data security in cloud computing and examined the drawbacks associated with data leakages or breaches in this field. However, failed to address the issue of how sensitive data can be leaked and compromised in cloud computing, as well as the solutions to these data leakage problems.

The authors in [22] thoroughly analyzed various aspects of cloud computing, including architectures, service models, deployment models, cloud components, and security issues. However, they did not delve into the existing solutions found in the literature for the identified security concerns. The authors discussed cloud security issues that can occur when data is moved within the cloud. The effectiveness of the lightweight directory access protocol (LDAP), public key infrastructure (PKI), and the role of a trusted third party (TTP) in ensuring the availability, authenticity, confidentiality, and integrity of data during communications was a topic of heated debate. The authors in [23] conducted a thorough qualitative analysis of vulnerabilities and the corresponding threats in each service model. They also suggested measures to improve security in cloud computing. The authors in [23] primarily emphasize the vulnerabilities and the threats that arise from them. The authors failed to address future research directions and current challenges arising from the identified vulnerabilities and threats.

The authors in [24] noticed a gap in the literature regarding the mapping of security issues to their solutions. They also recognized the importance of a common framework to generalize this idea and conducted a thorough analysis of specific needs. The authors also touched upon the open problems and potential areas for future research. The authors in [25] conducted a comprehensive literature review to identify the existing research on resource scheduling and security in the cloud. The authors in [25] classified various threats and explored potential solutions in the existing literature.

The authors in [26] discussed the security challenges of cloud computing, different types of cloud, and various service models of cloud computing. The author presented a comprehensive analysis of cloud challenges and future research directions in [26] based on the existing literature. The authors in [27] emphasized the importance of addressing security issues in cloud computing, which is a shared concern for both cloud service providers and users. The authors effectively tackled the issue of cloud security by acknowledging the importance of security requirements and offering viable solutions to mitigate potential threats. The authors in [28] highlighted the significance of having a comprehensive understanding of security issues pertaining to processes, people, and technology. The authors categorized cloud security issues into three main areas: processes, people, and technology. Threats in these areas were also divided among managers and security divisions in order to address the security issues.

DL has achieved significant success in various domains of cloud computing, including biomedical data analysis, speech recognition, and image recognition [29,30,31,32]. DL enables the transformation of data into more abstract expressions and higher levels. DL architectures are structured as multi-layer neural networks. Assuming the data is already in high dimension. The data can be transformed into low quality by training different neural networks (NN) with a thin central layer to reconstruct the high dimension data input [33]. The proposal suggests that enhancing the intrinsic characterization of the data can lead to improved classification or data visualization. Through the use of comprehensive data, functions can be broken down into simpler components, facilitating a better understanding of their structures. A remarkable discovery was made by [34] regarding the learning abilities of the artificial neural network's multiple layers. The authors of this study highlighted the layer-by-layer "pretraining" procedure as a potential solution for addressing the problem of optimizing weights in nonlinear auto-encoders.

The authors in [35] explored the data security challenges faced by a developing country, specifically Nepal, in 2019. The study highlighted the various challenges encountered by developing countries, including issues related to confidentiality, charging models, breaches, segregation, access, integrity, security, storage, data center operation, service level agreements, costing models, and locality. The research findings highlighted storage, virtualization, and networks as significant security concerns. The authors in [36] conducted an analysis of the security protection method for public cloud based on the existing security threats and put forward their own security protection methods.

The researchers approached the study of security issues in cloud computing from a unique perspective. In today's fast-paced world, it is crucial to quickly identify security issues and challenges that arise due to the ever-changing nature of clouds. Several survey papers have highlighted concerns related to cloud architecture, while others have categorized security issues into three main areas: people, processes, and technology. Others have primarily addressed data security and privacy concerns or have provided a broader analysis of security issues. It is important to emphasize and tackle emerging security issues in the cloud computing domain.

3. Framework and Architecture of CC

This section provides an architecture description of cloud computing (CC), elucidating the framework and fundamental concepts that underpin the system. The purpose is to facilitate the analysis of security challenges, vulnerabilities, and threats across various network layers.

3.1. Cloud Computing and Its Fundamental Attributes

The cloud, like the Internet, is a pervasive network whose internal workings, including infrastructure and communications, are not visible to end users. The delivery of computing, memory, networks, and applications via the internet platform and from a data center is the objective of computing. The fundamental attributes of cloud computing, as delineated by the NIST definition, are illustrated in Figure 3. The following five characteristics are outlined in the NIST definition of cloud computing [37, 38].

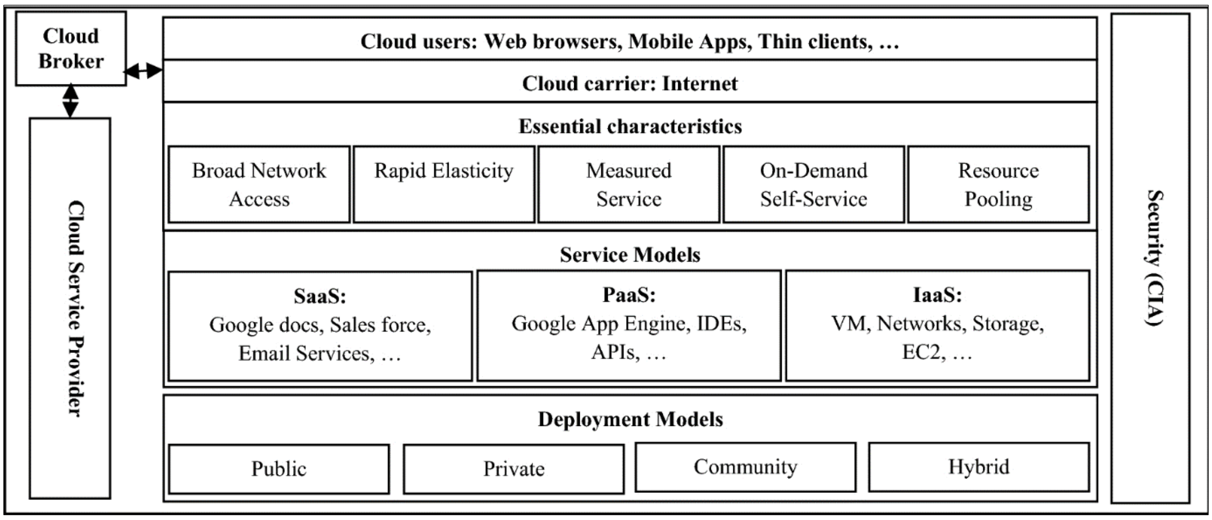
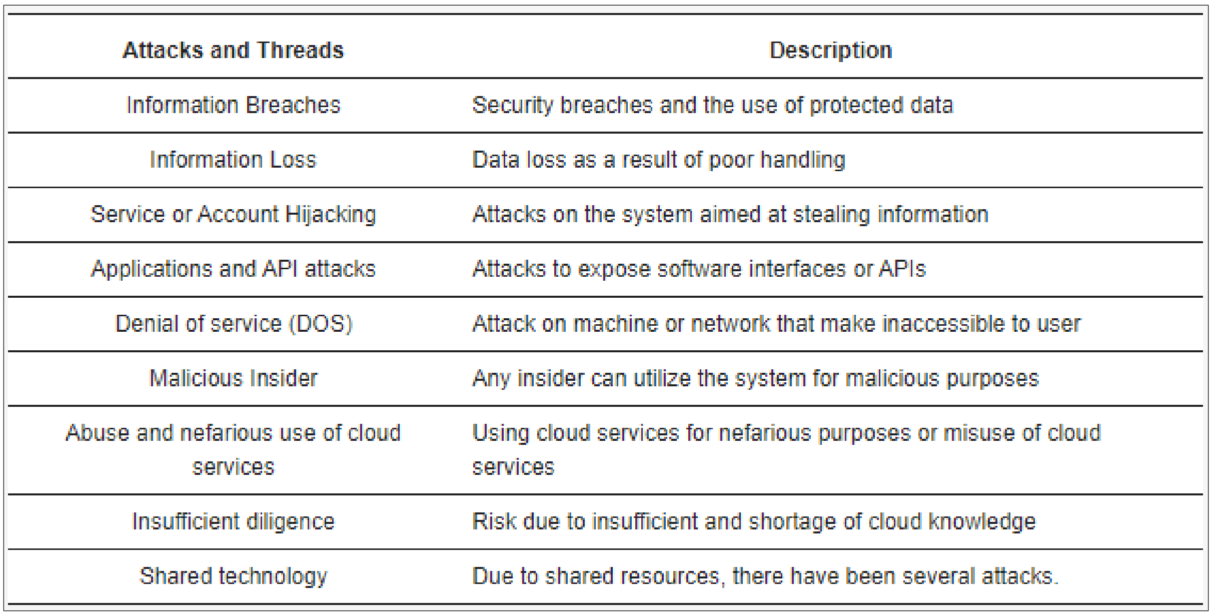


Figure 3 Cloud computing architecture as defined by NIST, drawing on references [37, 38, 39, 40]

- Demand-based self-service: Users can utilize the necessary resources in the cloud without human intervention. In order to facilitate this, cloud users are provided with an intuitive interface for managing their services and utilizing the resources.
- Wideband network connectivity: Standard devices, including laptops, desktop computers, and mobile phones, are capable of accessing the data and services hosted in the cloud through protocols that are native to these devices and are supported by the cloud environments.
- Resource aggregation: Cloud-based applications and programs require resources to function. In a shared environment, these resources are virtualized and dynamically assigned in accordance with the needs of the cloud users, despite their disparate physical locations. This mechanism conceals the location of the resource from the user.
- Irregular Elasticity: The resources are scalable in accordance with the needs of the users, and they are incentivized to utilize the cloud's infinite resources for a fee.
- Service Metrics: As a result of cloud computing's service-oriented architecture, the user's utilization of cloud resources can be dynamically assigned and evaluated. Consequently, users are required to remunerate for the resources they request.

4. IoT Based Cloud Attacks

Threats to data security in the cloud posed by the Internet of Things (IoT) rank high among concerns about using cloud services. Essentially, it's because a third-party vendor stores and processes the user's information invisibly. Bad authentication, stolen passwords, hacked accounts, data breaches, and other problems are in the news every day. As part of an interoperable system, cloud computing is employed to house data generated by IoT. In the cloud, users have constant and unrestricted access to a shared pool of computing resources. The internet of things generates massive data packets, and cloud computing provides a practical means of transporting them. When it comes to the IoT, scenario detection now requires the combination of data, as opposed to the physical linkages between web sites in the old internet. Figure 4 displays the traits of cloud attacks that are based on the IoT.



Attacks and Threads	Description
Information Breaches	Security breaches and the use of protected data
Information Loss	Data loss as a result of poor handling
Service or Account Hijacking	Attacks on the system aimed at stealing information
Applications and API attacks	Attacks to expose software interfaces or APIs
Denial of service (DOS)	Attack on machine or network that make inaccessible to user
Malicious Insider	Any insider can utilize the system for malicious purposes
Abuse and nefarious use of cloud services	Using cloud services for nefarious purposes or misuse of cloud services
Insufficient diligence	Risk due to insufficient and shortage of cloud knowledge
Shared technology	Due to shared resources, there have been several attacks.

Figure 4 Analyzed and characterized cloud threats based on the IoT (Adopted from [1])

4.1. Account Hijacking

This type of attack involves the unauthorized access and control of an individual or organization's cloud account by an intruder. The attacker for future attacks often utilizes the stolen account information, with the individual or organization becoming the primary target. The potential consequences of an attacker's actions can be severe, resulting in the unauthorized disclosure of sensitive information and significant damage to one's reputation [41]. Figure 5 provides a visual representation of this attack. Businesses and organizations have the opportunity to implement simple yet effective measures to ensure the security of their data in the cloud. Here are a few straightforward solutions to safeguard against cloud account hijacking:

- Make sure to check with your service provider to ensure that the workers who have physical access to the server have undergone background checks.
- Ensure a dependable authentication strategy for cloud application clients.
- Prevent access to cloud apps by disabling specific IP addresses.

Users can specify IP ranges in several cloud applications, allowing them to access the app using the company network or VPN.

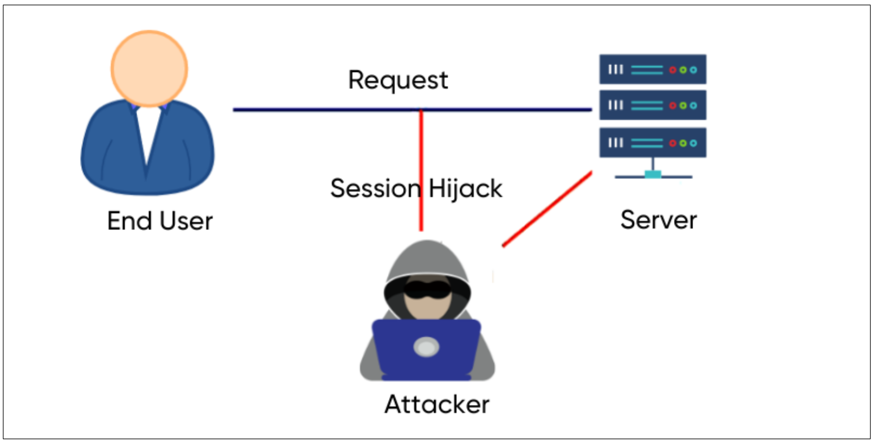


Figure 5 Account Hijacking

4.2. Denial of Service (DoS) Attacks

IoT systems are frequently targeted by denial of service attacks due to their prevalence and ease of implementation. This type of attack on the cloud can have serious consequences. In this scenario, the attacker deliberately blocks access to services, applications, or data for the intended user [42]. This attack is executed by overwhelming a specific machine, application, or service with a high volume of requests. As a result, the regular traffic becomes difficult to handle, causing a denial-of-service for other users. Figure 6 depicts a graphical representation of the denial of service attack. This type of attack is driven by the desire to push the cloud service owner to increase elasticity levels and utilize more virtual resources to handle the surge in traffic. The ultimate result is a disregard for responsibility and the quality of service (QoS). In addition, denial of service can serve as a catalyst and be utilized as a diversion to hide the malicious activities that bypass the cloud firewall. As a result, it can rapidly spread and cause greater harm instead of just impacting a single device [43]. DoS attacks aim to hinder users from accessing IoT, cloud networks, and other computer services. An IoT denial of service (DoS) attack aims to disrupt a system or network, making it inaccessible to its intended users.

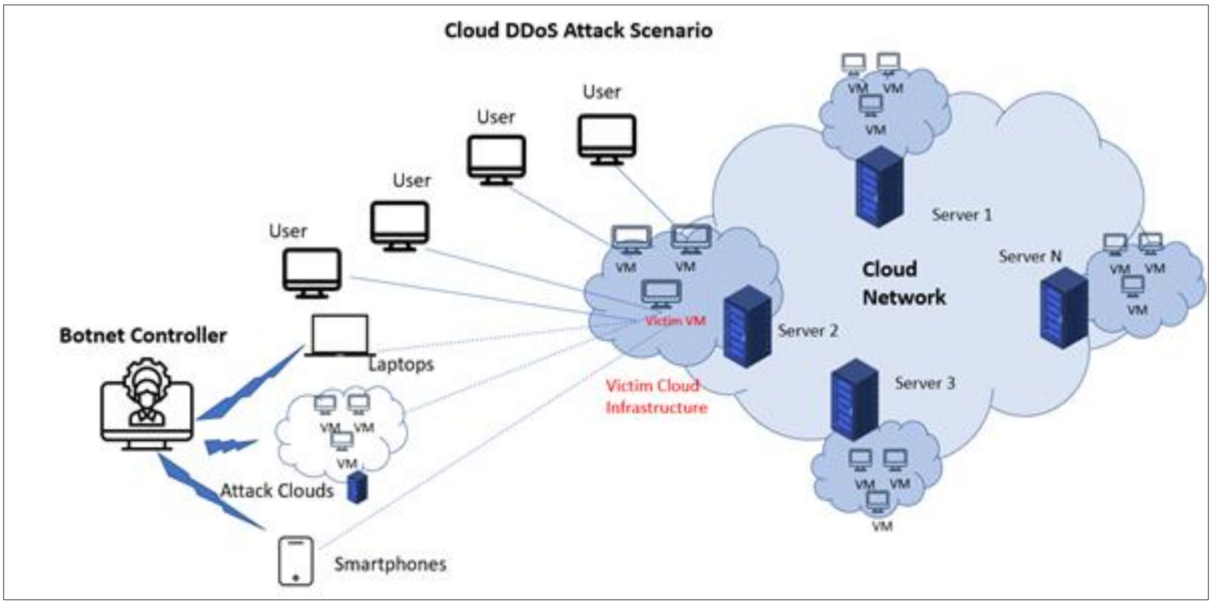


Figure 6 Cloud DDoS Attack Scenario

4.3. Phishing Attacks

Phishing attacks targeting cloud service providers entice customers by sharing a document or photo, prompting them to check in using their account credentials in order to obtain access. In this type of attack, the perpetrators send phishing emails with the intention of gathering personal or corporate account login information and accessing confidential data. This allows them to obtain a strategic advantage in executing the assault while avoiding discovery. Phishing attacks can manifest in two forms inside a cloud computing environment. There are two methods used by attackers. The first method involves stealing accounts using traditional social engineering tactics. The second method involves abusive conduct, where the attacker uses cloud services to host a phishing attack site.

4.4. Malware Injection Attacks

During a malware injection assault, the assailant attempts to introduce harmful programs and services into the cloud infrastructure. The assailant employs many techniques to execute this assault, while considering the cloud model. Initially, the assailant generates a malevolent service application module or a virtual machine instance and endeavors to incorporate it into the cloud. Subsequently, the assailants endeavor to transform it into a legitimate occurrence, subsequently diverting the requests of the legitimate user to the malevolent service application, and carrying out the malevolent code.

5. Challenges in Security for Client and Server Layers of CC

In this section we present a concise overview of the key security challenges faced by the client and server layers of cloud computing. Ensuring the privacy and confidentiality of data transmitted between clients and servers is a persistent challenge. Addressing potential breaches and unauthorized access demands robust encryption mechanisms and secure communication protocols.

5.1. Security Challenges of CSP

Ensuring the security and privacy of user data is a top priority for CSPs. The lack of transparency in the provision of cloud services hinders users from fully benefiting from these services. It is crucial for CSPs to incorporate effective access control methods, establish robust security policies to mitigate potential risks, offer logfile requests, and ensure transparency in the SLA. The CSP typically provides SLAs, and users must verify and approve the relevant agreement before using cloud services. It is important to ensure that these agreements are compiled, approved, and implemented at various levels in all aspects of cloud services. The security attachment of this agreement should address important security features, including reliability, integrity, data integrity, and high availability of the provided services. In this subsection, we have compiled a list of the common security challenges that can arise in the client and server layers due to CSP.

5.1.1. Offering Vulnerable APIs to Cloud Users

CSP offers a range of APIs that allow users to interact with cloud services [51, 52]. The security of these APIs is crucial for ensuring the safety and access privileges of users to the cloud services. This threat may impact all three main cloud service models [53]. These APIs are used to conduct authentication, access control, encryption, and monitoring of activities. It is important for cloud users to monitor APIs and prioritize their security in the SLA. API security is crucial in safeguarding against any malicious attempts to bypass user interfaces.

5.1.2. Insufficient awareness

The CSP ensures that cloud users are promptly notified of any security events that occur in the cloud environment. This allows users to stay updated on the status of their physical assets (such as servers, switches, routers, storage, etc.) as well as their intangible assets (such as data, databases, etc.). The CSP should be responsible for reporting various security incidents, such as online attacks and information theft. Otherwise, the CSP is found guilty. It is important to include the topic of informing security events, along with other security services, in the text of the SLA.

5.1.3. Restricting Cloud Users to a Single CSP

One of the challenges faced by cloud users is the limitation of using the services of only one provider. This challenge has the potential to impact all three main service models of the cloud. As an illustration, in the case of IaaS, the user might encounter difficulties when attempting to migrate their VMs to a different provider's cloud infrastructure. Transferring software to a new provider's platform may not be possible in PaaS. Transferring data to a new provider may not be a straightforward process for cloud users in the SaaS industry. It is advisable for cloud users to only migrate their non-critical applications to cloud environments offered by different providers.

5.1.4. Insufficient Service Provisioning by the CSP

The inability of CSP to continue operating poses challenges for users who migrate to the cloud in search of its computing benefits. They may encounter difficulties in finding a new provider and face compatibility issues with their software, data, or virtual machines. Deploying to multiple CSPs is crucial for ensuring high availability of the cloud user's most important applications.

5.1.5. Account Theft

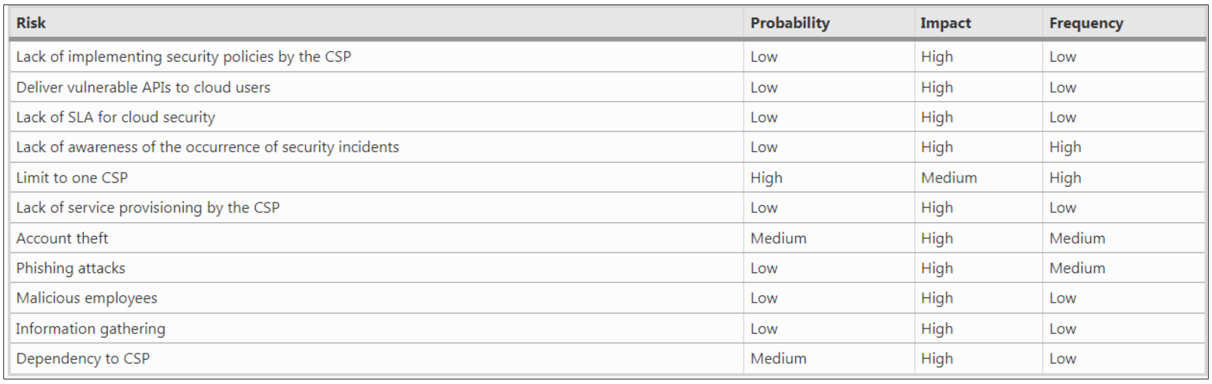
Account theft involves deceptive tactics used by hackers to falsely assume the identity and credibility of a legitimate user, as well as access their related resources and benefits. This threat can arise from various factors such as weak passwords, phishing attacks, and unauthorized access to encryption keys. This threat has the potential to impact all three main cloud service models.

Possible solutions

- Implementing robust multi-factor authentication mechanisms.
- Utilizing intricate passwords
- It is important to use the secure HTTPS protocol when communicating with the provided services of the cloud environment.

5.2. Assessing the Risks of Security Challenges in the Client and Server Layers of CC

The security challenges of the client and server layers of the cloud are thoroughly evaluated in three levels, utilizing the Delphi method. Figure 7 presents the probability of occurrence, the impact of challenges during their occurrence, and the frequency of occurrence for security challenges in the cloud client and server layers.



Risk	Probability	Impact	Frequency
Lack of implementing security policies by the CSP	Low	High	Low
Deliver vulnerable APIs to cloud users	Low	High	Low
Lack of SLA for cloud security	Low	High	Low
Lack of awareness of the occurrence of security incidents	Low	High	High
Limit to one CSP	High	Medium	High
Lack of service provisioning by the CSP	Low	High	Low
Account theft	Medium	High	Medium
Phishing attacks	Low	High	Medium
Malicious employees	Low	High	Low
Information gathering	Low	High	Low
Dependency to CSP	Medium	High	Low

Figure 7 The occurrence, consequences, and frequency of security breaches at the client and server layers of the cloud [54-61]

6. Conclusion

IoT cloud platforms bring extra security and privacy risks, according to this research. Researchers may focus on these cloud computing system areas: Security concerns: Researchers may study the latest cloud security models and present their analysis, focus on more security issues in current cloud systems, and provide different logical control techniques to improve cloud security. They may also review existing security issues and challenges in cloud computing, such as authenticity, encryption, multi-tenancy, virtual machine security, and how to reduce them.

The recent decade has seen businesses, companies, and hackers transform by adopting cloud technology. Modern cloud designs, high-speed internet, and new developments posed cloud computing security risks. This cloud technology change gave a business freedom and scalability to innovate and compete in the ever-changing industrial environment. However, it rendered their data less secure and attackable for various reasons. The article covered cloud designs, deployment methodologies, and prevalent threats.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Ahmad W, Rasool A, Javed AR, Baker T, Jalil Z. Cyber Security in IoT-Based Cloud Computing: A Comprehensive Survey. Electronics. 2022; 11(1):16.

[2] Mohiyuddin, A.; Javed, A.R.; Chakraborty, C.; Rizwan, M.; Shabbir, M.; Nebhen, J. Secure Cloud Storage for Medical IoT Data using Adaptive Neuro-Fuzzy Inference System. Int. J. Fuzzy Syst. 2021, 1–13.

[3] Karam, Y.; Baker, T.; Taleb-Bendiab, A. Security support for intention driven elastic cloud computing. In Proceedings of the 2012 Sixth UKSim/AMSS European Symposium on Computer Modeling and Simulation, Malta, Malta, 14–16 November 2012; pp. 67–73.

[4] Ibtisum, S. (2020). A Comparative Study on Different Big Data Tools

[5] Abid, R.; Iwendi, C.; Javed, A.R.; Rizwan, M.; Jalil, Z.; Anajemba, J.H.; Biamba, C. An optimised homomorphic CRT-RSA algorithm for secure and efficient communication. Pers. Ubiquitous Comput. 2021, 1–14.

[6] Mell, P.; Grance, T. The NIST Definition of Cloud Computing; Special Publication (NIST SP) Series; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2011.

[7] S M Atikur Rahman, Sifat Ibtisum, Ehsan Bazgir and Tumpa Barai. The Significance of Machine Learning in Clinical Disease Diagnosis: A Review. International Journal of Computer Applications 185(36):10-17, October 2023.

[8] S M Atikur Rahman, Sifat Ibtisum, Priya Podder and S. M. Saokat Hossain. Progression and Challenges of IoT in Healthcare: A Short Review. International Journal of Computer Applications 185(37):9-15, October 2023.

[9] Sifat Ibtisum, Ehsan Bazgir, S M Atikur Rahman, S. M. Saokat Hossain, "A comparative analysis of big data processing paradigms: Mapreduce vs. apache spark", World Journal of Advanced Research and Reviews, 20(01), 1089–1098, 2023.

[10] S M Atikur Rahman, Iqtiar Md Siddique, Eric D Smith, "Analyzing bitcoin's decentralization: Coefficient of variation approach and 21 million divisibility" Advancement of IoT in Blockchain Technology and its Applications, Vol. 2, Issue: 3, pp. 8-17, 2023.

[11] Bharati, S., Podder, P., Mondal, M. R. H., & Paul, P. K. (2021). Applications and challenges of cloud integrated IoMT. Cognitive Internet of Medical Things for Smart Healthcare: Services and Applications, 67-85.

[12] Ghobaei-Arani, M.; Souri, A.; Baker, T.; Hussien, A. ControCity: An autonomous approach for controlling elasticity using buffer Management in Cloud Computing Environment. IEEE Access 2019, 7, 106912–106924

[13] C. D. Martino, S. Sarkar, R. Ganesan, Z. T. Kalbarczyk and R. K. Iyer, "Analysis and Diagnosis of SLA Violations in a Production SaaS Cloud," in IEEE Transactions on Reliability, vol. 66, no. 1, pp. 54-75, March 2017, doi: 10.1109/TR.2016.2635033.

[14] Su, J. Why Cloud Computing Cyber Security Risks Are On The Rise: Report. Forbes. 25 July 2019. Available online: https://www.forbes.com/sites/jeanbaptiste/2019/07/25/why-cloud-computing-cyber-security-risks-are-on-the-rise-report/#13a36bfc5621. (accessed on 1 Decemeber 2023).

[15] Mishra, P.; Negi, A.; Pilli, E.; Joshi, R. VMProtector: Malign Process Detection for Protecting Virtual Machines in Cloud Environment. In Third International Conference on Advances in Computing and Data Sciences, ICACDS 2019, Ghaziabad, India, April 12–13, 2019, Revised Selected Papers, Part I; Springer: Singapore, 2019; pp. 360–369.

[16] Khorshed, M.T.; Ali, A.S.; Wasimi, S.A. A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing. Future Gener. Comput. Syst. 2012, 28, 833–851.

[17] Sifat Ibtisum, S M Atikur Rahman, S. M. Saokat Hossain, "Comparative Analysis of MapReduce and Apache Tez Performance in Multinode Clusters with Data Compression", World Journal of Advanced Research and Reviews, 2023.

[18] Ismail, N. Cursing the cloud (or) controlling the cloud? Comput. Law Secur. Rev. 2011, 27, 250–257.

[19] King, N.J.; Raja, V. Protecting the privacy and security of sensitive customer data in the cloud. Comput. Law Secur. Rev. 2012, 28, 308–319.

[20] Ryan, P.; Falvey, S. Trust in the clouds. Comput. Law Secur. Rev. 2012, 28, 513–521

[21] Singh, A.; Chatterjee, K. Cloud security issues and challenges: A survey. J. Netw. Comput. Appl. 2017, 79, 88–115.

[22] Mushtaq, M.F.; Akram, U.; Khan, I.; Khan, S.N.; Shahzad, A.; Ullah, A. Cloud computing environment and security challenges: A review. Int. J. Adv. Comput. Sci. Appl. 2017, 8, 183–195.

[23] Singh, A. Security concerns and countermeasures in cloud computing: A qualitative analysis. Int. J. Inf. Technol. 2019, 11, 683–690.

[24] Basu, S.; Bardhan, A.; Gupta, K.; Saha, P.; Pal, M.; Bose, M.; Basu, K.; Chaudhury, S.; Sarkar, P. Cloud computing security challenges & solutions-A survey. In Proceedings of the 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 8–10 January 2018; pp. 347–356.

[25] Sheikh, A.; Munro, M.; Budgen, D. Systematic Literature Review (SLR) of resource scheduling and security in cloud computing. Int. J. Adv. Comput. Sci. Appl. 2019, 10.

[26] An, Y.; Zaaba, Z.; Samsudin, N. Reviews on security issues and challenges in cloud computing. In IOP Conference Series: Materials Science and Engineering; IOP Publishing: Bristol, UK, 2016; Volume 160, p. 012106.

[27] Wani, A.R.; Rana, Q.; Pandey, N. Analysis and countermeasures for security and privacy issues in cloud computing. In System Performance and Management Analytics; Springer: Singapore, 2019; pp. 47–54.

[28] Ghaffari, F.; Gharaee, H.; Arabsorkhi, A. Cloud Security Issues Based on People, Process and Technology Model: A Survey. In Proceedings of the 2019 5th International Conference on Web Research (ICWR), Tehran, Iran, 24–25 April 2019; pp. 196–202.

[29] Chan, T.H.; Jia, K.; Gao, S.; Lu, J.; Zeng, Z.; Ma, Y. PCANet: A simple deep learning baseline for image classification? IEEE Trans. Image Process. 2015, 24, 5017–5032.

[30] Graves, A.; Mohamed, A.r.; Hinton, G. Speech recognition with deep recurrent neural networks. In Proceedings of the 2013 IEEE international conference on acoustics, speech and signal processing, Vancouver, BC, Canada, 26–31 May 2013; pp. 6645–6649.

[31] Hinton, G.; Deng, L.; Yu, D.; Dahl, G.E.; Mohamed, A.R.; Jaitly, N.; Senior, A.; Vanhoucke, V.; Nguyen, P.; Sainath, T.N.; et al. Deep neural networks for acoustic modeling in speech recognition: The shared views of four research groups. IEEE Signal Process. Mag. 2012, 29, 82–97.

[32] Liang, M.; Li, Z.; Chen, T.; Zeng, J. Integrative data analysis of multi-platform cancer data with a multimodal deep learning approach. IEEE/ACM Trans. Comput. Biol. Bioinform. 2014, 12, 928–937.

[33] Li, P.; Li, J.; Huang, Z.; Li, T.; Gao, C.Z.; Yiu, S.M.; Chen, K. Multi-key privacy-preserving deep learning in cloud computing. Future Gener. Comput. Syst. 2017, 74, 76–85.

[34] Hinton, G.E.; Salakhutdinov, R.R. Reducing the dimensionality of data with neural networks. Science 2006, 313, 504–507.

[35] Giri, S.; Shakya, S. Cloud Computing and Data Security Challenges: A Nepal Case. Int. J. Eng. Trends Technol. 2019, 67, 146–150.

[36] Wu, W.; Zhang, Q.; Wang, Y. Public Cloud Security Protection Research. In Proceedings of the 2019 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC), Dalian, China, 20–22 September 2019; pp. 1–4.

[37] Mell, P., &Grance, T. (2011). The NIST Definition of Cloud Computing. In NIST Special Publication, 800–145.

[38] Brandao P (2019) Cloud computing security. Interdisciplinary Center for History, Cultures and Societies (UID/HIS/00057/2019), pp 1–32

[39] Liu F, Tong J, Mao J, Bohn R, Messina J, Badger L, Leaf D (2011) NIST cloud computing reference architecture. In: NIST special publication, pp 500–292

[40] Jangjou, M., Sohrabi, M.K. A Comprehensive Survey on Security Challenges in Different Network Layers in Cloud Computing. Arch Computat Methods Eng 29, 3587–3608 (2022). https://doi.org/10.1007/s11831-022-09708-9

[41] Riaz, S.; Khan, A.H.; Haroon, M.; Latif, S.; Bhatti, S. Big Data Security and Privacy: Current Challenges and Future Research perspective in Cloud Environment. In Proceedings of the 2020 International Conference on Information Management and Technology (ICIMTech), Bandung, Indonesia, 13–14 August 2020; pp. 977–982.

[42] Iwendi, C.; Rehman, S.U.; Javed, A.R.; Khan, S.; Srivastava, G. Sustainable Security for the Internet of Things Using Artificial Intelligence Architectures. ACM Trans. Internet Technol. (TOIT) 2021, 21, 1–22.

[43] Harkut, D.G. Introductory Chapter: Cloud Computing Security Challenges. In Cloud Computing Security-Concepts and Practice; IntechOpen: London, UK, 2020

[44] Sarker, B., Sharif, N. B., Rahman, M. A. & Parvez, A. S. (2023). AI, IoMT and Blockchain in Healthcare. Journal of Trends in Computer Science and Smart Technology, 5(1), 30-50. doi:10.36548/jtcsst.2023.1.003.

[45] Mondal MRH, Bharati S, Podder P, Kamruzzaman J. Deep Learning and Federated Learning for Screening COVID-19: A Review. BioMedInformatics. 2023; 3(3):691-713.

[46] S. Bharati, M. R. H. Mondal and P. Podder, "A Review on Explainable Artificial Intelligence for Healthcare: Why, How, and When?," in IEEE Transactions on Artificial Intelligence, doi: 10.1109/TAI.2023.3266418.

[47] Podder, P., Mondal, M., Bharati, S., & Paul, P. K. (2021). Review on the security threats of internet of things. arXiv preprint arXiv:2101.05614.

[48] Bharati, S., Mondal, M., Podder, P., & Prasath, V. B. (2022). Federated learning: Applications, challenges and future directions. International Journal of Hybrid Intelligent Systems, 18(1-2), 19-35.

[49] Bharati, S., Mondal, M. H., Khamparia, A., Mondal, R. H., Podder, P., Bhushan, B., ... & Kumar, S. (2021). 12 Applications and challenges of AI-driven IoHT for combating pandemics: a review (pp. 213-230). Berlin, Boston: De Gruyter.

[50] Robel, M. R. A., Bharati, S., Podder, P., & Mondal, M. R. H. (2020). IoT driven healthcare monitoring system. Fog, Edge, and Pervasive Computing in Intelligent IoT Driven Applications, 161-176.

[51] Singh A, Chatterjee K (2017) Cloud security issues and challenges: a survey. J Netw Comput Appl 79:88–115

[52] Almutairy M, Al-Shqeerat HA, Al Hamad H (2019) A taxonomy of virtualization security issues in cloud computing environments, pp 1–19

[53] Swathy Akshaya M, Padmavathi G (2019) Taxonomy of security attacks and risk assessment of cloud computing, pp 37–59

[54] Amundrud Y, Aven T, Flage R (2017) How the definition of securityrisk can be made compatiblewith safety definitions. Proc IMechE Part O J Risk Reliab 231:3

[55] Aven T (2012) The riskconcept—historical andrecentdevelopmenttrends. Reliab Eng Syst Saf 99:33–44

[56] Macher G, Armengaud E, Brenner E, Kreiner C (2016) Threat and risk assessment methodologies in the automotive domain. Proc Comput Sci. https://doi.org/10.1016/j.procs.2016.04.268

[57] Nurse, J., Creese, S., Roure, D. (2017). Security risk assessment in Internet ofThings systems, Article to be published in IT Professional (IT Pro), September/October 2017 Special Issue on “Establishing Trust in the Internet ofThings”

[58] Sajko M, Rabuzin K, Bača M (2006) How to calculate information value for effective security risk assessment. J Inf Org Sci 30:2

[59] Wangen G (2017) Information security risk assessment: a method comparison. IEEE Comput Mag Spec Issue Cyber Phys Syst Secur Risk Assess 50(4):52–61

[60] Bharati, S., Mondal, M. R. H., Podder, P., & Kose, U. (2023). Explainable Artificial Intelligence (XAI) with IoHT for Smart Healthcare: A Review. Interpretable Cognitive Internet of Things for Healthcare, 1-24.

[61] Ahmmed, S.; Podder, P.; Mondal, M.R.H.; Rahman, S.M.A.; Kannan, S.; Hasan, M.J.; Rohan, A.; Prosvirin, A.E. Enhancing Brain Tumor Classification with Transfer Learning across Multiple Classes: An In-Depth Analysis. BioMedInformatics 2023, 3, 1124-1144. https://doi.org/10.3390/biomedinformatics3040068.